Disaster Recovery and Business Application

- National Medicaid HIPAA and MMIS Conference
- February 12, 2003
- presented by Maryland Medical Care Programs, Brenda Rose

HIPAA Privacy requires: Safeguards 164.530(c)

- *A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.*
- *A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart*

Safeguards, continued

- Covered entities are to maintain safeguards adequate for their operations;
- Safeguards are to be flexible and scalable;
- Safeguards are to cover all protected health information for both paper and electronic;
- Role-based access rules needed for "minimum necessary" and uses and disclosures of PHI.

Administrative Procedures:A covered entity is required to implement "documented, formal practices" to manage PHI

- Certification
- Chain of Trust Agreements
- Contingency Plan
- Formal Mechanism for record processing
- Information access control
- Internal Audit
- Personnel Security
- Security Configuration Management
- Security Incident Process
- Security Management Process
- Termination Procedures
- Training

Administrative Procedures

- These practices are to include a Contingency Plan-described as “a routinely updated plan for responding to a system emergency, that includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster.”

Contingency Plan

- A Contingency Plan must include:
  - analysis/assessment of the sensitivity, vulnerabilities and security of the covered entities programs and information;
  - Data backup plan
  - A disaster recovery plan
  - Emergency mode operation plan
  - Testing and Revision procedures

The Disaster Recovery Plan

- A component of the contingency plan
- Contains the information and a documented process describing how:
  - a covered entity will be able to continue to conduct business
  - a covered entity can recover the information.

Disaster Recovery Plan

- Attempts to determine the impact on business functions if a disaster occurred;
- Defines resources, tasks and data required to recover our business functions;
- Establishes the predetermined level of functioning needed to meet our goals of recovery.

Challenges in developing Disaster Recovery Plans

- Analysis is extensive and time consuming
- Details are built on assumptions
- Assumptions are made on predicting the type(s) of event that creates the disaster
- Staff dedication and resource allocations to the plan are massive
- Effective communication

Elements of Our Disaster Recovery Plan

- Plans were created for each of the major business functions that we identified were strategic to continue:
- Claims
- Pharmacy POS
- Enrollment
- Eligibility Verification
- Hotlines

Objectives of our plan

- Strategy: rely on current staff, temporary staff; rely on performance of critical functional and reporting processing until normal operations can be done.
- Implementation mode: identification where manual replacement and semi automatic processes can be implemented
- Affected systems: list of all systems and subsystems
- Assumptions: elements the plan is based on such as telephone, electricity, water, physical location

Outputs and services

- Essential Functions: drill down to the basics
- Required outputs and services: what is the goal
- Affected Stakeholders: who has the greatest risk
- Notification Procedure: how do we tell others

Criteria for Invoking the plan

- Determine what event triggers the plan to go into effect
- Specific as to who will determine to what degree the plan is to be implemented

Roles, Responsibilities and Authority

- Business Contingency Plan Organization: describes the type of staff to be involved
- Delegation of Authority: determines who takes the lead
- Emergency Response Team/ Business Resumption Team: lists members of team, contact numbers
- Common Infrastructure Elements: describes authority process over shared information/systems
- Security: what standards can be implemented until usual business resumes
- Communication: “real time” status reporting process, documentation of events

Expected Life of the Plan

- Plan Life: initial life of the plan - until such time as the function is no longer considered a core business function
- Operational Life: how long the plan will be in effect dependent upon the exact nature of the event.

Resource Constraints

- Partners and Agency Interfaces: list of primary business partners
- Public Infrastructure Services: services provided such as electricity, water, telephones
- Key resources: staffing and training needed to

Training and Testing

- Training exercises: joint effort among all involved staff
- Training schedule: predetermined schedule for testing the plan
- Plan validation: utilizing manual review and desktop exercises (unable to perform actual simulation)
- Plan monitoring: review of plan validity

Procedures for Invoking Disaster Recovery Plan

- Implementation Strategy: process for determining which part of the plan is needed dependent on projected durations
- Recovery Procedures: definition of levels of priority
- Manual Processes: description of the manual processes and procedures

Procedures for Operating in Contingency Mode

- Contingency Plan steps: identification of key steps that must be executed to minimize loss and begin recovery
- Duration: attempt to establish the impact of duration on the level of plan needed
- Emergency Items/ Alternated Work Sites
- Reporting Procedures: Establish hierarchy for reporting
-

Other Elements to consider:

- Resource plan for Operating Plan: time, cost, staff, other resources
- Criteria for returning to Normal Operations
- Procedures for returning to Normal Operations
- Recovering Lost or Damaged Data

Benefits, despite the labor

- Forces staff to share with others what they do and how, provides for greater awareness
- Increased awareness allows people to develop a sense of ownership and commitment to the process
- Often, staff who are aware are more likely to participate in more preventative actions

Discussion

Thank you.